

FILED

OCT 07 2014

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

STEPHEN C. WILLIAMS
U.S. MAGISTRATE JUDGE
SOUTHERN DISTRICT OF ILLINOIS
EAST ST. LOUIS OFFICE

IN THE MATTER OF THE SEARCH OF)
)
CONTENT OF, AND RECORDS)
RELATING TO, E-MAIL ACCOUNT)
"LEEDOERR87@GMAIL.COM")
WHICH ARE STORED AT PREMISES)
OWNED, MAINTAINED, CONTROLLED,)
OR OPERATED BY GOOGLE, INC.)

CASE NUMBER 14-mj-7082

**APPLICATION AND AFFIDAVIT
FOR SEARCH WARRANT**

I, Karla F. Heine, being duly sworn depose and say:

I am a Special Federal Officer (SFO) with the Federal Bureau of Investigation's (FBI) Springfield Child Exploitation Task Force (SCETF), and have reason to believe that the

**content of, and records relating to, e-mail account
"leedoerr87@gmail.com"**

constitutes evidence of the commission of a criminal offense or which is contraband, the fruits of crime, or things otherwise criminally possessed; all in violation of Title 18, United States Code, Sections 2252 and 2252A, specifically evidence related to the transportation, distribution, receipt and/or possession of child pornography. The facts to support the issuance of a search warrant are as follows:

AFFIDAVIT

1. I am a SFO with the FBI assigned to the SCETF based in the FBI's Springfield Division, Fairview Heights, Illinois, Resident Agency. The SCETF is an FBI sponsored Task Force assembled to combat a variety of cyber-related crime in the Metro East area, and is comprised of law enforcement personnel from approximately fifteen (15) different local, state, and federal agencies.

I have been assigned to the SCETF for approximately seven (7) years. My primary employment is as a sworn police officer for the Columbia Police Department, a position I have held for approximately 19 years. During this time, I have conducted and assisted in the investigation of state and federal offenses including the possession, receipt and transmission of images of child pornography and other sexual offenses against children. I have gained knowledge, experience, and training in such investigations through training seminars, classes, and work with other state and federal cyber-crime investigators. I have learned about the habits of child pornography collectors, distributors, and producers, those who exploit children online, and those who commit sexual offenses against children. I have been trained in the search and recovery of computers and peripherals, in the extraction of computer data and data from cellular telephones, and in the forensic preview of computers located at a suspect's residence. I have had the opportunity to observe and review numerous examples of child pornography, as defined in 18 U.S.C. §2256(8)(A) and (C), in all forms of media including computer media.

2. I am a federal law enforcement officer with the authority to execute warrants issued under the authority of the United States, and make this affidavit in support of an application under Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) for a search warrant for information associated with the **content of, and records relating to, e-mail account "leedoerr87@gmail.com" (hereinafter "SUBJECT ACCOUNT")** which are stored at premises owned, maintained, controlled, or operated by Google, Inc. (hereinafter "Google"), an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. As set forth more fully below, there is probable cause to believe that someone has used the **SUBJECT ACCOUNT** to transport, distribute, receive and/or possess child pornography, in violation of Title

18, United States Code, Sections 2252 and 2252A.

3. The search warrant sought in this application would require Google to disclose to the Government records and other information in its possession, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNT**, including the contents of any wire and/or electronic communications.

4. The statements contained in this affidavit are based upon my training and experience as a Special Federal Officer and Detective of the Columbia Police Department, Special Agents with the FBI, as well as other law enforcement officers and investigators, and upon my consultation with personnel trained in the investigation, seizure, and analysis of electronic data and electronic media. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, United States Code, Sections 2252 and 2252A exist in the **SUBJECT ACCOUNT** which are stored at premises owned, maintained, controlled, or operated by Google, an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ELECTRONIC SERVICE PROVIDERS

1. Although they are under no legal obligation to do so, Electronic Service Providers (ESPs), like Microsoft, typically monitor their online networks for child pornography. Due to the large number of files uploaded to their servers each day, ESPs routinely rely on hash value comparisons to identify child pornography files.

2. A hash value is essentially the unique digital signature of a file. Hash values come in different forms and can be produced by a variety of digital algorithms. The Secure Hash

Algorithm (SHA), for instance, was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), for use with the Digital Signature Standard (DSS) as specified within the Secure Hash Standard (SHS). The United States of America has adopted the SHA as a Federal Information Processing Standard. A file processed by the SHA results in the creation of an associated hash value that is unique to the contents of that file. SHA signatures provide a certainty exceeding 99.99 percent that two or more files with the same SHA value are identical copies of the same file, regardless of their file names.

3. ESPs typically maintain digital libraries of hash values known to be associated with suspected child pornography files. These libraries consist of hash values belonging to files that have previously been opened, viewed, and subjectively deemed by someone to contain child pornography. Some hash values may be added to the library by the ESP, while others may be acquired from other entities.

4. When an ESP finds a file on its network with a flagged hash value, it means that the contents of a file with the same hash value were previously viewed by someone and determined by that person to contain child pornography.

5. Electronic service providers, electronic communication services, and remote computer service providers are mandated, pursuant to Title 18, United States Code, Section 2258A, to report all facts or circumstances from which there is an apparent violation of federal child pornography laws to the National Center for Missing and Exploited Children ("NCMEC") Cyber Tipline.

GOOGLE/GMAIL

1. Google provides a variety of on-line services, including e-mail access to the general

public. Subscribers obtain an account by registering with Google's GMAIL's email service. During the registration process, Google/GMAIL asks subscribers to provide basic personal information. Therefore, the computers of Google/GMAIL are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Google/GMAIL subscribers) and information concerning subscribers and their use of Google/GMAIL services, such as account access information, e-mail transaction information, and account application information.

2. In general, an e-mail that is sent to a Google/GMAIL subscriber is stored in the subscriber's "mail box" on Google/GMAIL servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google/GMAIL servers indefinitely.

3. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google/GMAIL's servers, and then transmitted to its end destination. Google/GMAIL often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google/GMAIL server, the e-mail can remain on the system indefinitely.

4. A Google/GMAIL subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Google/GMAIL.

5. Subscribers to Google/GMAIL might not store copies of the e-mails stored in their Google/GMAIL account on their home computers. This is particularly true when they access their Google/GMAIL account through the web or if they do not wish to maintain particular e-mails or files in their residence.

6. In general, e-mail providers like Google Inc/GMAIL ask each of their subscribers to

provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

7. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google/GMAIL's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

8. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

GOOGLE DRIVE

1. Google Drive is a file storage and synchronization service provided by Google/GMAIL which enables user cloud storage. Google Drive stores a person's documents,

photos, videos, and other files on Internet servers rather than the person's hard drive. A person can access those files from any computer, smartphone or tablet with an Internet connection. Google Drive gives 15 GB of free storage and then allows access to purchase more storage. Google Drive allows people to share files with others. Files or folders can be shared privately with particular users having a Google account, using their @gmail.com email addresses. Sharing files with users not having a Google account requires making them accessible to "anybody with the link." This generates a secret URL for the file which may be shared via email, blogs, etc. Files and folders can also be made "public on the web" which means that they can be indexed by search engines and thus can be found and accessed by anyone.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

1. Based upon my knowledge, training, and experience, I am aware that child pornography distributors/collectors:

a. Receive sexual gratification, stimulation, and satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (in person, in photographs, or other visual media) or from literature describing such activity.

b. Collect sexually explicit or suggestive materials (hard-core and soft-core pornography, whether of adults and/or of children) in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

c. Almost always possess and maintain their material (pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings,

child erotica, etc.) in the privacy and security of their homes or some other secure location. Child pornography distributors/collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years, and store their child pornography amongst other, otherwise legal, media or files.

d. Often correspond and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

e. Often maintain their collection of child pornography in computer files located on a computer hard drive or other computer media and that these computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache". The

browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

f. Files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files. In addition, computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of internet service accounts used to access the Internet.

PROBABLE CAUSE STATEMENT

1. On December 27, 2013, Tumblr, Inc., notified the National Center for Missing and Exploited Children (NCMEC) that thirty-four (34) possible images of child pornography had been uploaded to the "Tumblr.com" network by a computer with IP address 70.195.64.46. Tumblr identified the images as suspected child pornography by their hash values and subsequently shut down the account. Tumblr informed NCMEC that the person using IP address 70.195.64.46 had the following URL address: "http://loveteenspuss.tumblr.com," the user name "loveteenspuss" and that the email address associated with the account was "buddy_lee34@hotmail.com."

2. On January 16, 2014, NCMEC forwarded the cyber-tip to the Illinois Attorney General's Crimes Against Children Task Force (ICAC), who subsequently forwarded it to the FBI's

SCETF. The information from NCMEC came in the form of a password protected e-mail labeled Cyber Tipline Report #2245550 which contained the thirty-four (34) image files uploaded by "http://loveteenspuss.tumblr.com," with the user name "loveteenspuss," and e-mail address "buddy_lee34@hotmail.com." The IP address associated with these uploads was 70.195.64.46. A search was conducted through Facebook for the e-mail address, buddy_lee34@hotmail.com, and returned to the following the Facebook account https://www.facebook.com/lee.doerr31. This account belongs to Lee Doerr from Dupu, Illinois. ICAC sent an email to SFO Dave Vucich on March 29, 2014, which he then forwarded to me on April 4, 2014, regarding this criminal activity.

3. On April 21, 2014, a subpoena was sent to Microsoft Online Services requesting subscriber information for "buddy_lee34@hotmail.com." The subpoena return indicated that the email address belonged to Lee Doerr from Illinois, 62239, and was registered on August 6, 2002. On May 1, 2014, the case was assigned to me to begin a criminal investigation into Doerr's online activities.

4. On May 27, 2014, I obtained a federal search warrant to view the thirty-four (34) image files that had been uploaded to the Tumblr.com network by Doerr. When I executed the search warrant, I found that, based on my training and experience, seventeen (17) of the images were of minors engaged in sexually explicit conduct, some of whom were prepubescent; eight (8) of the image files were blank; five (5) images appeared to be of minors engaged in sexually explicit conduct but because of the position of the minor or the camera, it was too difficult to make a definite determination; three (3) images that involved minors that did not meet the federal definition of child pornography; and one (1) image of adult pornography.

5. A search of the name Lee Doerr in the Consolidated Lead Evaluation and Reporting

site, otherwise known as Clear, reported that Richard L. Doerr, II, lived at 2135 Mullins Creek Road, Dupo, Illinois. The report also indicated that Richard L. Doerr, III, date of birth 1987, also lived at this address. Finally, the report also provided a phone number of (618) 830-0246 in connection with the Doerrs.

6. A subpoena was sent to Verizon Wireless requesting the subscriber name, address, billing address, and length of service for the IP address (70.195.64.46) used during the uploading of the images of child pornography to the "Tumblr.com" network on December 27, 2013. The subpoena also requested records of session times and duration for Internet connectivity during the time of the download. Verizon's response to the subpoena indicated that IP address 70.195.64.46 is a Nating Router IP. Nating routers are used by the phone companies to provide internet access to multiple phone lines at the same time. Verizon attached a report containing all of the phone numbers that utilized the particular Nating Router IP during the time the images of child pornography were uploaded to the "Tumblr.com" network on December 27, 2013. The phone number associated with the Doerrs -- 618-830-0246 -- was one of the telephone numbers used during that time frame. A check of this telephone number revealed that it is registered to Richard L. Doerr, II, date of birth 1962, and has been active since July, 2004.

7. Another open source search was conducted of Lee Doerr's Facebook account. Profile pictures posted on his Facebook account matched the driver's license picture of Richard L. Doerr, III, which provided a date of birth of 1987 (hereinafter "DOERR"). This Facebook account is used almost daily, with the last time being October 2, 2014.

8. On October 2, 2014, I, FBI Special Agent Joseph Murphy, FBI SFO Jason Robertson and FBI Special Analyst Derek Valazco went to 2135 Mullins Creek Road, Dupo, Illinois, to

conduct a knock and talk. Upon arrival, Special Agent Murphy and I met with DOERR's father (hereinafter "Mr. Doerr") who told us that DOERR had not lived with him for approximately two years, but that he still received many of his bills at his residence. Mr. Doerr stated that DOERR's current cellular telephone was in his (Mr. Doerr's) name, and had the number 618-830-0246. Mr. Doerr tried to call DOERR but there was no answer. Mr. Doerr did not know DOERR's street address but did provide us with directions to DOERR's residence.

9. We followed the directions provided by Mr. Doerr, and soon arrived at 2333 Old State Route 3, Apartment B, East Carondelet, Illinois 62240, within the Southern District of Illinois. Special Agent Murphy knocked on door which was answered by DOERR. DOERR gave permission for all of the agents to enter his residence.

10. When asked about his Tumblr account, DOERR admitted being the sole user of two Tumblr accounts, "loveteenspuss" and "Leezy87." DOERR also admitted sharing child pornography photos on both of his Tumblr accounts. He said that, around December 2013, he began using the "loveteenspuss" account to share child pornography but was blocked by Tumblr and the account was shut down. DOERR said that the email address, buddy_lee34@hotmail.com, was associated with the "loveteenspuss account," as well as his Facebook account, Lee Doerr. He said that, around May 2014, he created another Tumblr account named "Leezy87," and shared some child pornography photos using this account. DOERR said that he was blocked by Tumblr again and the account was shut down.

11. DOERR said that he also created a Kik Messenger account using the user name "Leezy87." He said that he shared child pornography pictures with other users through his Kik Messenger account. DOERR reported that, when he received the photographs depicting child

pornography, he would save them to the Google Drive associated with the **SUBJECT ACCOUNT**.

DOERR provided the account name and password for the Google Drive associated with his **SUBJECT ACCOUNT** as follows: username "leedoerr87@gmail.com" (the **SUBJECT ACCOUNT**) and password "bellaharley." DOERR also signed a Consent to Assume Online Presence Form allowing law enforcement agents to take over control of the **SUBJECT ACCOUNT** and the Google Drive associated with the **SUBJECT ACCOUNT**.

12. DOERR said that mainly used his cellular phone, 618-830-0246, and his Samsung Tablet, to share images of child pornography. DOERR stated that, most of the time, he used the Wi-Fi from his cellular telephone to access an Internet connection, but that on September 25, 2014, he obtained a wireless router through Charter Communications.

13. Finally, DOERR stated that, in approximately July 2014, he communicated with a thirteen (13) year old minor female on Kik messenger. DOERR admitted asking the minor for some pictures, and stated that she sent him some photographs of her breasts and vagina. Doerr also admitted that he sent the thirteen (13) minor photographs of his penis.

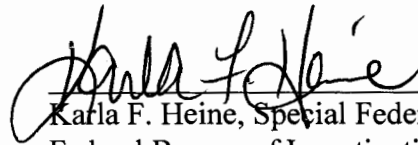
14. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the **SUBJECT ACCOUNT** there exists evidence of a crime and contraband or fruits of a crime. Specifically, DOERR indicated that he kept his images of child pornography on the Google Drive associated with the **SUBJECT ACCOUNT**. Accordingly, a search warrant is requested.

15. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the Government copies of the records and other

information (including the content of communications) pertaining to the **SUBJECT ACCOUNT**, as set forth in Attachment A.

16. This Court has jurisdiction to issue the requested warrant because it is “a court with jurisdiction over the offense under investigation.” 18 U.S.C. §2703(a).

FURTHER AFFIANT SAYETH NAUGHT.



Karla F. Heine, Special Federal Officer
Federal Bureau of Investigations

STEPHEN R. WIGGINTON
United States Attorney

ANGELA SCOTT
Assistant United States Attorney

State of Illinois)
) SS
County of St. Clair)

Sworn to before me, and subscribed in my presence on the 7th day of October, 2014, at
East St. Louis, Illinois.


STEPHEN C. WILLIAMS
United States Magistrate Judge

ATTACHMENT A
PARTICULAR THINGS TO BE SEIZED

Google, Inc., is required to disclose the following information related only to the **SUBJECT ACCOUNT**:

1. All subscriber information for the **SUBJECT ACCOUNT**;
2. The content of all opened and unopened messages or other correspondence involving the **SUBJECT ACCOUNT**;
3. All images or videos associated with the **SUBJECT ACCOUNT**, and all text, quotes, links, and audio files associated with the **SUBJECT ACCOUNT**;
4. Any accounts that “liked” or “re-blogged” posts made by the **SUBJECT ACCOUNT**;
5. All accounts the **SUBJECT ACCOUNT** followed;
6. All friends or contact lists, and all followers of the **SUBJECT ACCOUNT**;
7. All groups or pages the **SUBJECT ACCOUNT** was a member of;
8. All comments posted on the **SUBJECT ACCOUNT** and all comments posted by the **SUBJECT ACCOUNT**;
9. All histories or log files associated with the **SUBJECT ACCOUNT**, including connection dates and times, methods of connection (telenet, ftp, http, smtp), and IP addresses of the source of the connection;
10. All methods of payment and detailed billing records;
11. All privacy settings and other user-controlled settings associated with the **SUBJECT ACCOUNT**;
12. All records pertaining to communications between Google, Inc., and any person regarding the **SUBJECT ACCOUNT**, including contacts with support services and records of actions taken;
13. All records, image files and/or video files relating to the exploitation of children, child pornography, crimes against children, or a sexual interest in children; and
14. All records relating to who created, used, or communicated with the **SUBJECT ACCOUNT**.